Information Systems
Cybersecurity CAE-2Y
Associates of Applied Science Degree

61 credit hours (All Online)

The Associates of Applied Science in Information Systems (IS) Cybersecurity is designed to introduce students to contemporary information systems security, information assurance and demonstrate how these systems are used throughout global organizations. The focus of this program will be on the key components of information systems assurance and cybersecurity - people, software, hardware, data, security, and communication technologies, and how these components can be integrated and managed to create competitive advantage. ***The National Security Agency and the Department of Homeland Security have designated Eastern New Mexico University - Ruidoso as a National Center of Academic Excellence in Information Assurance/Cybersecurity (CAE-2Y)***. This program is specifically designed to prepare students in the National Initiative In Cybersecurity Education (NICE) Framework for Operate and Maintain and Protect and Defend or provide current Information Systems professionals with an Information Systems security certification to meet the needs of current and future employer requirements. The program maps to a Cybersecurity Technician job position based on NICE framework. Upon completion of this program students will receive a university certification of completion, the CompTIA Security+ and EC - Council Certified Ethical Hacker (CEH)™ industry certification in addition to their degree. Key is that the program meets the CAE-2Y curriculum certification by the NSA and complies with the DOD 8570 certification. The students will participate in the Cybersecurity Challenge Competition with industry partners to demonstrate and apply program knowledge in the capstone class.

Upon program completion students will be able to:

- Apply capable skills to plan, analyze, develop, implement, maintain, and enhancing information systems security programs, policies, procedures, and tools to ensure the confidentiality, integrity, and availability of systems, networks, and data.
- Understand and apply knowledge to implement higher-level security requirements; integrate security programs across disciplines; define security plans and policies; assess new system design methodologies to improve software quality; and institute measures to ensure awareness and compliance.
- Knowledge to evaluate and assess new security technologies and/or threats and recommend changes; review and evaluate security incident response policies; and develop long-range plans for IT security systems.

- Understanding and knowledge to resolve integration issues related to the implementation of new systems with the existing infrastructure and why information systems are used today and the technology, people, and organizational components of information systems.
- Understand and analyze various types of information systems provide the information needed to gain business intelligence to support the decision making for the different levels and functions of the organization, the value of information systems investments, how organizations develop and acquire information systems and technologies.as well as learn to formulate a business case for a new information system, including estimation of both costs and benefits.
- Understand, apply and evaluate how to secure information systems resources, mitigate risks as well as plan for and recover from disasters, focusing on both human and technological safeguards, ethical concerns that information systems raise in society, and the impact of information systems on crime, terrorism, and war.

Prerequisites:
None

Institutional and Related Course Requirements – 14 hours

UNIV 101 – Freshman Seminar – 3
MATH 104 – Preparatory Algebra – 4
MGT 201 – Principles of Management – 3
STAT 213 – Statistical Methods I – 4

New Mexico General Education Common Core (NMECC) 19 hours

Area I. Communications – 9 hours

Required courses -
COMM 101 – Interpersonal Communications – 3
ENG 102 – English Composition – 3
ENG 233 – Writing for Technical Professionals – 3

Area II. Mathematics – 3 hours

Required Course -
MATH 119 – College Algebra – 3

Area III. Science – 4 hours

Recommended courses:
BIOL 113 – Biology for General Education/Lab - 4
BIOL 154/L – General Biology: Subcellular through Organismic Biology/Lab – 4
BIOL 155/L – General Biology: Organismic through Supra Organismic Biology/Lab – 4
CHEM 113 – Chemistry for Today/Lab - 4
CHEM 151/L – General Chemistry I
CHEM 152/L – General Chemistry I Lab
Or any science with a lab listed in the NMECC

Area IV. Social Science – 3 hours

Recommended Courses:
PSCI 101 – Introduction to Political Science (NMCCNS POLS 1113) - 3
PSCI 102 – American National Government – 3
PSY 101 – Introductory Psychology – 3

SOC 101 – Introductory Sociology – 3
or a Social Sciences from the NMECC

Technical Requirements – 28 hours

CS 123/L – Programming Fundamentals/Lab – 4
IS 131 – Network Security Fundamentals – 3 (KU)
IS 136 – Guide to Disaster Recovery – 3 (KU)
IS 153 – Introduction of Information Systems – 3 (KU)
IS 160 – Overview of Operating Systems & Utilities – 3 **(KU)**
IS 253 – Firewalls and How They Work – 3
IS 257 – Ethical Hacking Network Defense and Counter Measures – 3 (KU)
IS 258 – Cyber Ethics, Professionalism, and Career Development – 3
IS 298 – Programmatic Capstone/Cybersecurity Challenge – 3

*Highlighted courses provide Computer and Network Security Certificate
KU - CAE/CDE mapped KU's

Title: CS 123/L – PROGRAMMING FUNDALMENTALS/LAB (4) Credits
Core Course
Catalog description
This class is a requirement for the Computer Technology, Associate of Applied Science degree. It is also useful for anyone interested in learning Programming Logic and Design fundamentals leading to programming. Students will become familiar with the fundamentals of programming logic and design, flow charting, pseudo code, Microsoft Visio Professional, and JAVA. Four credit hours. Concepts and programming technique fundamentals using JAVA to the practice and theory of Computer Science: I/O, operators and expressions, control structures, functions and arrays.

Objectives:

1. Understand and application of the basic fundamentals of programming structure.
2. Understand and application of modules, hierarchy charts, and documentation.
3. Understand and application of making decisions, looping, control breaks and arrays.
4. Understand and application of designing and writing a complete program.
5. Basic understanding and application of Notepad++, NetBeans IDE and JAVA.

Title: IS 131 COMPUTER AND SECURITY FUNDAMENTALS. (3) Credits
Core Course
Catalog description
A comprehensive overview of network security concepts that include: remote access, e-mail, the Web, directory and file transfer, wireless data, common network attacks, cryptography, operational/organizational security, disaster recovery, business continuity, and Cyber Ethics.

Objectives:

1. Differentiate and distinguish between the different network design elements, components, ports and protocols, their respective threats and mitigation techniques. (IS131)
2. Identify and apply industry best practices for access control methods. (IS131)
3. Deploy various authentication models and identify the components of each. (IS131)
4. Conduct periodic audits of system security settings and discuss how to improve analysis by auditing network security procedures and carry out vulnerability assessments using common tools. (IS131)
5. Use monitoring tools on systems and networks and direct security-related anomalies. (IS131)

6. Determine the appropriate use of network security tools to facilitate network security. (IS131)
7. Summarize the various authentication models and identify the components of each. (IS131)

Title: IS 136 GUIDE TO BUSINESS CONTINUITY AND DISASTER RECOVERY (3) Credits
Core Course
Catalog description
Presents methods to identify vulnerabilities and take appropriate countermeasures to prevent and mitigate failure risks for an organization. It will take an enterprise-wide approach to developing a disaster recovery plan.

Objectives:

1. Understand the key functions of the disaster plan and have the ability to implement disaster recovery procedures. (IS136) (IS131)
2. Define and explain information security, basic concepts of risk management and how to conduct risk assessments and implement risk mitigation. (IS131) (IS136)
3. Identify and define the components of contingency planning (IS136)
4. Know some of the concerns and trade-offs to be managed when assembling the final IR plan, understand the elements of an incident recovery response, and be aware of the impact of selecting a reaction strategy, developing a notification mechanism, and the creation of escalation guidelines (IS136)
5. Know and understand the relationships between the overall use of contingency planning and the subordinate elements of incident response, business resumption, disaster recovery, and business continuity planning (IS136)
6. Recognize what critical elements compose the response phase of the DR plan (IS136)
7. Know the methodology used to construct the business continuity policy and plan, and be able to participate in such a planning process when required (IS136)

Title: IS 153 Introductions (Foundations) of Information Systems (3) Credits
Core Course
Catalog description
Information systems are an integral part of all business activities and careers. This course is designed to introduce students to contemporary information systems and demonstrate how these systems are used throughout global organizations. The focus of this course will be on the key components of information systems - people, software, hardware, data, and communication technologies, and how these components can be integrated and managed to create competitive advantage. Through the knowledge of how IS provides a competitive advantage students will gain an understanding of how information is used in organizations and how IT enables improvement in quality, speed, and agility. This course also provides an introduction to systems and development concepts, technology acquisition, and various types of application software that have become prevalent or are emerging in modern organizations and society. Includes participating in the National Cyber League Competition.
Objectives:
1. Demonstrate understanding of history of computers, current computer technology and terminology. (IS153)
2. Understand computing disciplines: computer science and information systems. (IS153)
3. Understand networking and the Internet. (IS153)
4. Demonstrate knowledge of how technology is used in business. (IS153)
5. Understand Systems Development Life Cycle process. (IS153)
6. Understand some of the societal implications of computers and related technology. (IS153)
7. Understanding of INFOSEC processes and methodology and computer and network security..(IS153)

Title: IS 160 Overview of Operating Systems and Utilities (3) Credits
Core Course
Catalog description

This course is an overview of computer operating systems from PCs to mainframes. Including OS theory and structure as well as an introduction to systems control parameters, utilities, services and command language. Prerequisite: IS 153.
Objectives:

1. Understand Operating System Theory.(IS160)
2. Understand PC Operating System Hardware and interaction with the Operating System. (IS160)
3. Understand File Systems. (IS160)
4. Understand and apply Installing and Upgrading Operating Systems and hardware. (IS160)
5. Understand Network Connectivity and Resource Sharing Over a Network. (IS160)
6. Understand Standard Operating and Maintenance Procedures. (IS160)
7. Understand Virtual Operating Systems and applying that knowledge in administration and operations. (IS160)

Title: IS 253 FIREWALLS AND HOW THEY WORK (3) Credits
Core Course
Catalog description
This course introduces students to the design and implementation of firewalls. The course covers such topics as firewalls using CISCO Routers, Microsoft server platform and UNIX platform. Focuses on how firewalls function in these environments and the basic steps to plan and implement firewalls. PREREQUISITE: IS 131 or Instructor's permission.

Objectives:

1. Identify and implement different firewall configuration strategies and setup firewall rules that reflect an organizations overall security approach. (IS253)
2. Understand authentication, its criticality to network security, why and how firewalls authenticate users, the types of authentication groups, and the advantages and disadvantages of popular centralized authentication systems. (IS253)
3. Understand the various technologies that are used to implement detection and prevention. (IS253)
4. Know how firewalls work, misconceptions, and understand why a firewall is dependent on an effective security policy. (IS253)
5. Understand how proxy servers work and the goals an organization can achieve using a proxy server. (IS253)
6. Establish a set of rules and restrictions for a firewall and demonstrate the ability to support and maintain a firewall by updating, adhering to proven security principles, tracking logs, and following basic initial steps in response to security incidents. (IS253)
7. Understand the components and essential operations of virtual private networks (VPNs) and the different types and explain basic VPN concepts including encapsulation, encryption, and authentication in VPNs (IS253)

Title: IS 257 ETHICAL HACKING, COMPUTER AND NETWORK DEFENSE AND COUNTER MEASURES (3) Credits
Core Course
Catalog description
This course examines the tools, techniques and technologies used in the technical securing of information assets. Students will receive in-depth information about the software and hardware components of Information Security and Assurance. The students will experience an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter

defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council ANSI accredited Certified Ethical Hacker exam 312-50 PREREQUISITE: IS 131

Objectives:

1. Describe a layered approach to network defense, how to Manage firewalls to improve security, and explain the goal of securing the network perimeter and describe guidelines for auditing VPNs and VPN policies (IS257)
2. Identify the components of an intrusion detection system and explain the steps of intrusion detection, formulate a security policy and identify security policy categories (IS257)
3. Explain the Common Vulnerabilities and Exposures (CVE) standard, and explain the six-step incident response process (IS257)
4. Strengthen network control by managing security events (IS257)
5. Using Active and Passive Techniques to Enumerate Network Hosts, conducting Active and Passive Reconnaissance Against a Target, and breaking WEP and WPA Encryption
6. Using the SYSTEM account, and Poison Ivy – Remote Access Trojan, and Using the SHARK Remote Administration Tool and Utilizing Malware - Dark Comet
7. Using Spear Phishing to Target an Organization
8. Using Metasploit to Attack a Remote System, Using Armitage to Attack the Network, Exploitation with IPv6, and creating MSFPAYLOADS, Abusing SYSTEMS, SQL Injection, launching a Buffer Overflow, Intrusion Detection, and Using Certificates to Encrypt Email

Title: IS 258 CYBER ETHICS, PROFESSIONALISM, AND CAREER DEVELOPMENT (3) Credits
Core Course
Catalog description
This course exposes the student to the topic of Cyber Ethics, Professionalism, and Career Development. The course provides students seeking a career in Cyber Security insight on professional behavior required in a security job and how to develop a professional career in Cyber Security.

Objectives:

1. Understand the traditional ethical frameworks that can guide the student's analysis of the moral dilemmas and social problems that arise in cyberspace. (IS258)
2. Describe and understand the directive and architectonic role of moral ideals and principles in determining responsible behavior in cyberspace. (IS258)
3. Describe and understand the capacity of free and responsible human beings to exercise some control over the forces of technology. (IS258)
4. Explain and understand the appropriate regulatory response to social problems that have emerged in the online world and formulate and apply answer to the idea that market forces handle social problems or that the government intervention is essential. (IS258)
5. Understand and explain the bottom-up and top-down approaches to regulating the internet. (IS258)
6. Describe and formulate the optimal approach and interaction of regulatory policy and technology. (IS258)

7. Understand and apply career development processes and best practices.

IS 298-Fall: Programmatic Capstone/Cybersecurity Challenge Elective Course (3) Credits
Core Course
Catalog description

To offer engaging, entertaining, measurable, and scalable methods of learning to enlist a new generation of cybersecurity professionals. These games will be created and optimized for individuals and teams and are designed to provide hands-on experiences and challenges to help students to develop and improve cybersecurity skills and problem-solving abilities. All games will be conducted remotely, in virtual Cyber Stadiums, equally accessible to all. Prerequisites: Faculty Approval

Objectives:

1. Providing an inclusive individual and team competitive sport experience
2. Creating a fun, experiential learning opportunity where students demonstrate skills/knowledge sets
3. Promoting proficiency for specific cyber skills
4. Preparing teams for other cybersecurity exercises
5. Continuing the acquisition of skills tied to curriculum, industry needs, and professional certifications
6. Providing a mechanism by which schools/students can assess the effectiveness of their curriculum
7. Enriching the classroom learning experience
8. Successful completion of CompTIA Security + and EC - Council Certified Ethical Hacker (CEH)™ EXAMS